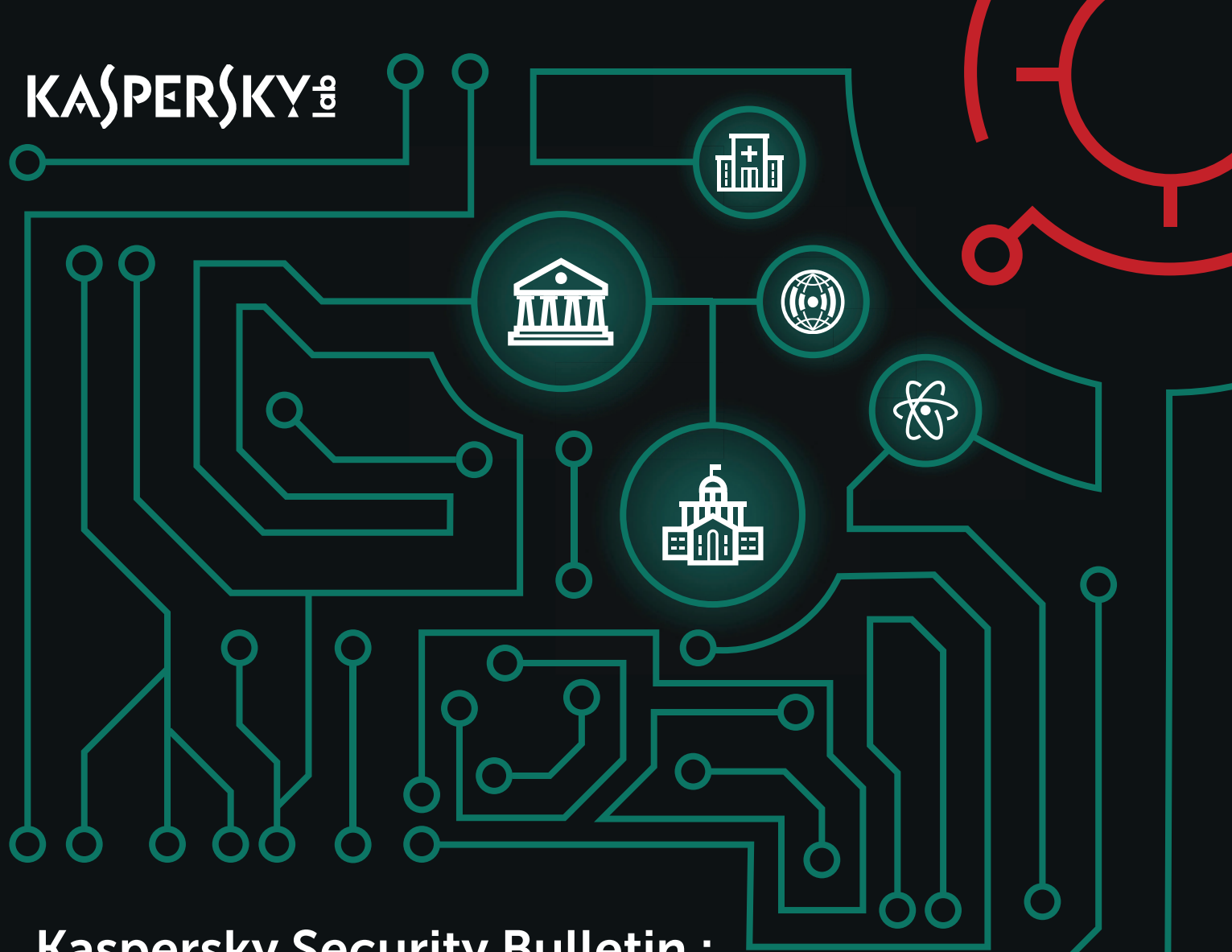
KASPERSKY lab



Kaspersky Security Bulletin :

PRÉVISIONS 2018 DES EXPERTS DE KASPERSKY LAB

SOMMAIRE

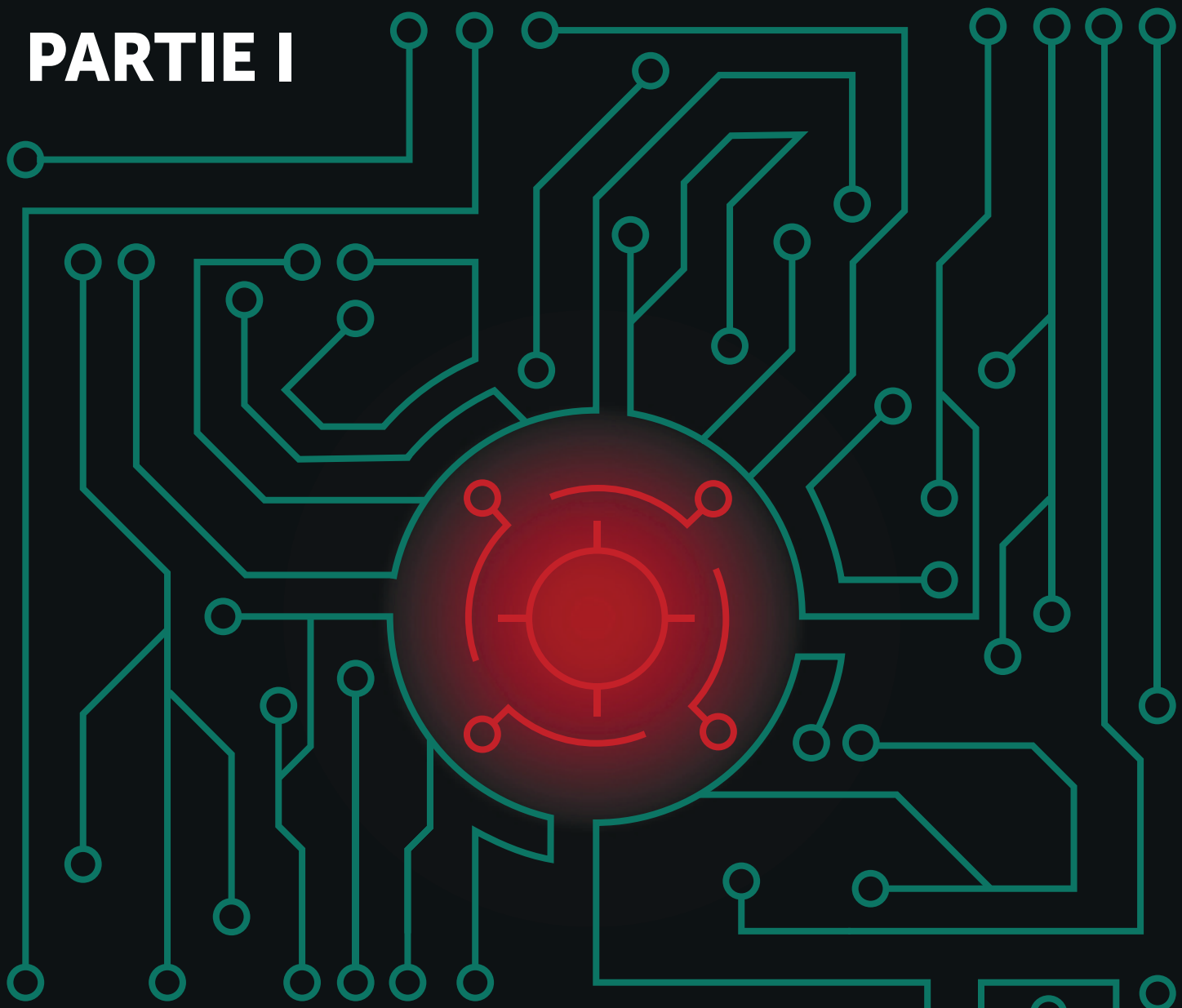
INTRODUCTION

En 2017, d'ingénieux cybercriminels ont continué à faire les gros titres en commettant des attaques et des vols audacieux, motivés par des raisons politiques. Mais cette année, ces événements ont dû partager la vedette dans les médias avec un autre type de menace, ciblant les entreprises de toutes tailles et se propageant à une vitesse à couper le souffle. Tout manquement en matière de sécurité réseau, de correctifs logiciels ou de sensibilisation des salariés a été impitoyablement mis en lumière, notamment lors de la vague d'attaques destructrices de ransomwares en mai et juin. Le coût final pour certaines entreprises a atteint des centaines de millions de dollars.

Pour répondre à la nécessité croissante qu'ont les entreprises de comprendre et de se préparer aux cybermenaces auxquelles fait face leur secteur, le Kaspersky Security Bulletin de 2018 comprend non seulement les prévisions de l'équipe Global Research and Analysis concernant les principales attaques ciblées, mais aussi une nouvelle section sur leurs prédictions pour différents secteurs industriels et technologiques.

Toutes nos prévisions sont fondées sur les recherches menées et l'expérience acquise par les experts de Kaspersky Lab au cours de l'année 2017. Nous les avons élaborées en tentant d'envisager au mieux ce que nous réserve l'avenir, sur la base nos connaissances actuelles. Nous espérons que ces éclairages susciteront la réflexion, la sensibilisation et vous aideront à mener vos actions de protection et de prévention pour l'année à venir.

PARTIE I



PRÉVISIONS : MENACES PERSISTANTES AVANCÉES

GREAT

INTRODUCTION

Une année comme 2017 témoigne du conflit interne des experts en sécurité : d'une part, chaque nouvel événement ouvre de nouvelles voies de recherche pour nous, car ce qui constituait autrefois un problème théorique s'exprime de façon palpable dans la réalité. Cela nous permet de comprendre la surface d'attaque et les tactiques réelles de l'attaquant, et d'affiner notre traque et nos techniques de détection afin de faire face aux nouvelles attaques. D'autre part, comme nous sommes particulièrement soucieux des systèmes de sécurité des utilisateurs d'une manière générale, chaque événement est plus catastrophique que le précédent. Plutôt que de considérer chaque nouvelle violation comme un simple nouvel exemple du même problème, nous percevons l'insécurité cumulée à laquelle font face aussi bien les utilisateurs que les acteurs de l'e-commerce et les institutions financières et gouvernementales.

Comme nous l'avons dit l'an dernier, plus qu'un argumentaire de vente à peine voilé, nos prévisions sont une tentative de mettre à profit les recherches que nous avons menées tout au long de l'année sous la forme de tendances susceptibles d'atteindre leur paroxysme au cours de l'année à venir.

NOS PRÉVISIONS PRÉCÉDENTES

Avions-nous vu juste ?

Telle une feuille de score montrant un aperçu de nos performances de l'an dernier, voici certaines de nos prévisions pour 2017 qui se sont avérées pertinentes :

Espionnage et menaces persistantes sophistiquées :

La mode des implants passifs ne montrant presque aucun signe d'infection – Oui !

Infections éphémères/programmes malveillants dans la mémoire – Oui !

L'espionnage s'attaque aux appareils mobiles - Oui !

Attaques financières :

L'avenir des attaques financières – Oui !

Ransomware :

Ces sales menteurs de ransomwares – Oui !

Menaces industrielles :

L'apocalypse pour les systèmes de contrôle industriel (SCI) n'a pas encore eu lieu (et nous sommes heureux d'avoir eu tort sur ce point), mais ces systèmes ont subi des attaques d'Industroyer – Oui !

Internet des objets :

Le botnet ciblé BrickerBot – Oui !

La guerre de l'information :

De multiples exemples - Oui !

À QUOI PEUT-ON S'ATTENDRE EN 2018 ?

Davantage d'attaques contre les chaînes d'approvisionnement

L'équipe Global Research and Analysis de Kaspersky Lab surveille plus de 100 opérations et groupes de menaces persistantes sophistiquées. Certains sont extrêmement sophistiqués et possèdent des arsenaux parmi lesquels des vulnérabilités « zero-day » ou des outils d'attaque sans fichier. D'autres consistent en des attaques de piratage traditionnelles qui passent le relai à des équipes plus sophistiquées chargées de l'exfiltration. Nous avons observé à de nombreuses reprises que des cybercriminels sophistiqués tentaient pendant longtemps d'atteindre une certaine cible sans y parvenir. Selon le cas, ces tentatives infructueuses s'expliquaient par le fait que la cible utilisait des suites de sécurité Internet fiables, avait formé ses salariés contre le piratage informatique ou suivait consciemment les stratégies des services de renseignement australiens pour atténuer les menaces persistantes sophistiquées.

En général, un cybercriminel considéré à la fois comme sophistiqué et persistant n'abandonne pas facilement ; il continue à tester les défenses jusqu'à trouver une brèche.

En l'absence de résultats, il est susceptible de prendre un peu de recul et de réévaluer la situation. Au cours d'une telle réévaluation, le cybercriminel peut arriver à la conclusion qu'une attaque de la chaîne d'approvisionnement pourrait être plus efficace que d'essayer d'accéder directement à sa cible. Même une cible dont les réseaux emploient les meilleures défenses au monde est susceptible d'utiliser des logiciels de tierces parties. De tels logiciels peuvent être des cibles plus faciles et être exploités pour attaquer l'entreprise cible d'origine.

Au cours de l'année 2017, nous avons observé plusieurs cas de ce genre, parmi lesquels, entre autres :

- Shadowpad
- CCleaner
- ExPetr / NotPetya

En 2018, nous nous attendons à voir davantage d'attaques sur les chaînes d'approvisionnement, autant en matière d'attaques découvertes que d'attaques latentes.

Ces attaques peuvent être extrêmement difficiles à identifier ou à atténuer. Par exemple, dans le cas de Shadowpad, les attaquants ont réussi à introduire un cheval de Troie dans un certain nombre de packages de Netsarang couramment utilisés dans le monde, dans les banques, les grandes entreprises et d'autres secteurs d'activité. La différence entre les packages propres et ceux infectés par un cheval de Troie peut être extrêmement difficile à percevoir ; dans de nombreux cas, c'est le trafic de commande et de contrôle (C&C) qui les trahit.

Pour CCleaner, il a été estimé que plus de 2 millions d'ordinateurs ont reçu la mise à jour infectée, ce qui en fait l'une des attaques les plus importantes de 2017. Une analyse du code malveillant de CCleaner nous a permis de faire la relation avec d'autres backdoors connus pour avoir été utilisés par le passé par des groupes de menaces persistantes faisant partie d'Axiom, comme APT17, aussi connu sous le nom d'Aurora. Cela prouve jusqu'où les groupes de menaces persistantes sophistiquées sont à présent disposés à aller pour atteindre leurs objectifs.

Nous pensons qu'il y a, à l'heure actuelle, sans doute beaucoup plus d'attaques sur les chaînes d'approvisionnement que celles que nous constatons, et que bon nombre d'entre elles n'ont pas encore été observées ou dévoilées. En 2018, nous nous attendons à voir davantage d'attaques sur les chaînes d'approvisionnement, autant découvertes que latentes. Introduire des chevaux de Troie dans des logiciels spécialisés utilisés dans des pays et des secteurs spécifiques sera comparable au fait de mener des attaques de point d'eau sur des sites choisis stratégiquement afin d'atteindre des groupes de victimes ciblés et s'avérera donc particulièrement alléchant pour certains types d'attaquants.

Davantage de programmes malveillants mobiles sophistiqués

En août 2016, CitizenLab et Lookout ont publié leur analyse de la découverte d'une plateforme d'espionnage de mobiles sophistiquée nommée Pegasus. Pegasus, qui est prétendument une suite logicielle « d'interception légale », est vendue à des gouvernements et à d'autres entités par une entreprise israélienne appelée NSO Group. Combinée à des vulnérabilités « zero-day » capables de contourner à distance les moyens de défense d'un système d'exploitation mobile moderne comme iOS, il s'agit d'une arme très puissante contre laquelle il n'y a pas grand-chose à faire. En avril 2017, Google a publié son analyse de la version Android du logiciel espion Pegasus, qu'il a baptisée Chrysaor. En plus des logiciels espions de « surveillance légale » tels que Pegasus et Chrysaor, de nombreux autres groupes de menaces persistantes sophistiquées ont élaboré leurs propres implants malveillants pour mobiles.

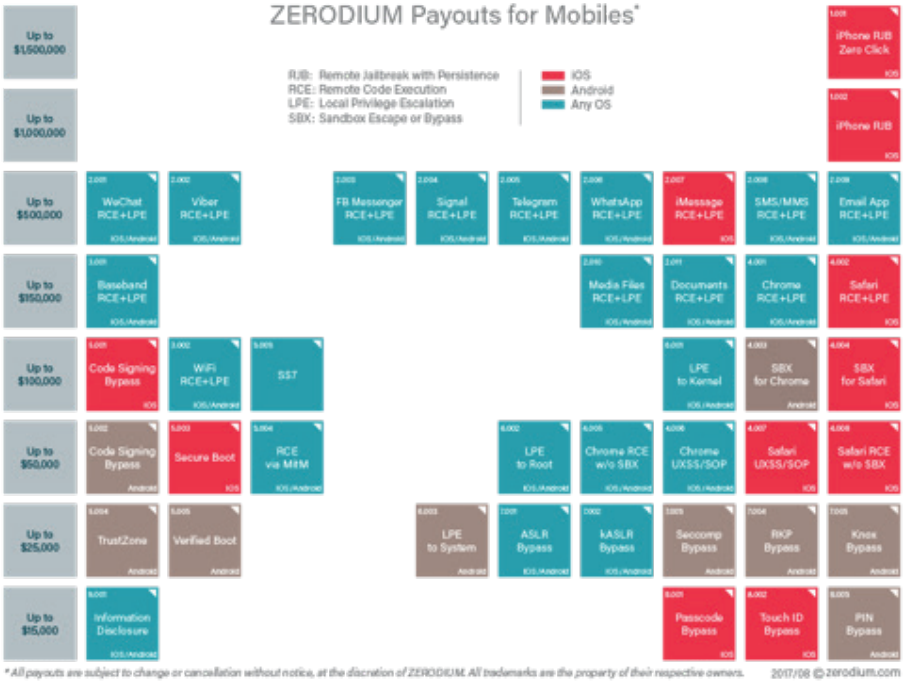
En 2018, davantage de programmes malveillants sophistiqués pour mobiles seront découverts, autant du fait d'une augmentation des attaques que de l'amélioration des technologies de sécurité.

Du fait qu'iOS est un système d'exploitation verrouillé contre les introspections, l'utilisateur ne peut pas faire grand-chose pour vérifier si son téléphone est infecté. Or, malgré la plus grande vulnérabilité d'Android, la situation est meilleure sur ce système d'exploitation où des produits tels que Kaspersky Internet Security for Android sont disponibles pour vérifier l'intégrité d'un appareil.

Nous pensons que le nombre total de programmes malveillants mobiles en circulation est probablement supérieur au nombre de signalements actuels en raison de lacunes de télémétrie qui les rendent plus difficiles à repérer et à éliminer. Nous estimons qu'en 2018, davantage de programmes malveillants sophistiqués pour mobiles seront découverts, autant du fait de l'augmentation des attaques que de l'amélioration des technologies de sécurité conçues pour les détecter.

Davantage de compromissions de type BeEF avec profilage Web

En raison d'un intérêt accru, d'une meilleure sécurité et de technologies d'atténuation déployées par défaut dans les systèmes d'exploitation, les tarifs des vulnérabilités « zero-day » ont grimpé en flèche en 2016 et 2017. Par exemple, le dernier tableau Zerodium mentionne des primes pouvant aller jusqu'à 1 500 000 $ pour un déverrouillage à distance complet sur iPhone (iOS) avec attaque persistante, autrement dit, une infection à distance sans interaction de l'utilisateur.



Les prix incroyables que certains clients gouvernementaux ont certainement choisi de payer pour ces vulnérabilités témoignent d'un intérêt de plus en plus élevé pour la protection de ces vulnérabilités contre toute divulgation accidentelle. Cela se traduit par la mise en œuvre d'une phase de reconnaissance plus solide avant de livrer les composants d'attaque réels. La phase de reconnaissance peut, par exemple, mettre l'accent sur l'identification des versions exactes du navigateur utilisé par la cible, son système d'exploitation, ses plug-ins et autres logiciels tiers. Armé de cette connaissance, le cybercriminel peut affiner sa tactique d'attaque et opter pour une vulnérabilité moins complexe, « 1-day » ou « N-day ».

L'utilisation de kits d'outils de profilage comme BeEF augmentera en 2018, et plus de groupes adopteront des frameworks publics ou développeront les leurs.

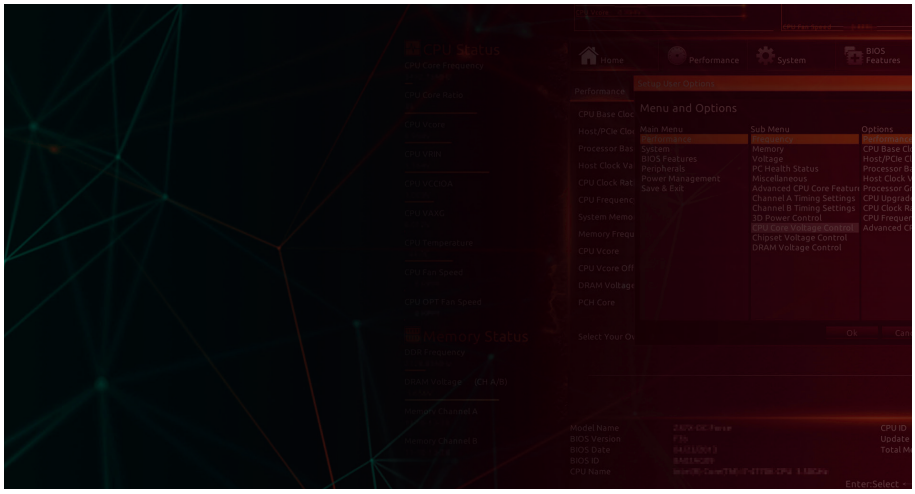
On retrouve souvent ces techniques de profilage chez les groupes de menaces persistantes sophistiquées comme Turla et Sofacy, ainsi que Newsbeef (aussi appelé Newscaster, équipe de piratage Ajax ou « Charming Kitten »), mais aussi chez d'autres groupes de menaces persistantes sophistiquées connus pour leurs frameworks personnalisés, tels que le prolifique Scanbox. Si l'on considère la popularité de ces frameworks avec les besoins en hausse en matière de protection des outils coûteux, nous prévoyons que l'utilisation de kits d'outils de profilage comme BeEF augmentera en 2018, et plus de groupes adopteront des frameworks publics ou développeront les leurs.

Attaques sophistiquées sur l'UEFI et sur le BIOS

En 2018, plus de programmes malveillants basés sur l'UEFI seront découverts.

L'UEFI (Unified Extensible Firmware Interface, interface micrologicielle extensible unifiée) est une interface logicielle qui sert d'intermédiaire entre le micrologiciel et le système d'exploitation sur des ordinateurs modernes. Créée en 2005 par une alliance des plus grands éditeurs de logiciels et développeurs de matériel, parmi lesquels Intel, elle est en train de rapidement remplacer le BIOS traditionnel. En effet, l'UEFI possède un certain nombre de fonctions avancées que le BIOS n'a pas : par exemple, la possibilité d'installer et d'exécuter des fichiers exécutables, des capacités réseau et Internet, la cryptographie, une architecture et des pilotes indépendants du processeur, etc. Les fonctions très évoluées qui font de l'UEFI une plateforme si attractive ouvrent également la voie à de nouvelles vulnérabilités qui n'existaient pas à l'ère du BIOS, plus rigide. Par exemple, la capacité de lancer des modules exécutables personnalisés permet de créer des programmes malveillants qui seraient exécutés par l'UEFI directement, avant que toute solution contre les programmes malveillants, ou avant que le système d'exploitation proprement dit, n'ait pu démarrer.

L'existence de programmes malveillants agissant sur l'UEFI est connue depuis 2015, lorsque les modules UEFI de Hacking Team furent découverts. Lorsqu'on sait cela, on peut trouver surprenant qu'aucun programme malveillant significatif affectant l'UEFI n'ait été trouvé, un fait que nous attribuons à la difficulté de détection de manière fiable. Nous prévoyons qu'en 2018, plus de programmes malveillants basés sur l'UEFI seront découverts.



Les attaques destructrices continuent

Kaspersky Lab observe depuis novembre 2016 une nouvelle vague d'attaques de wipers visant plusieurs cibles au Moyen-Orient. Le programme malveillant utilisé pour ces nouvelles attaques était une variante du ver tristement connu Shamoon qui avait ciblé Saudi Aramco et Rasgas en 2012. Sommeillant depuis quatre ans, l'un des plus mystérieux wipers de l'histoire est de retour. Aussi appelé Disttrack, Shamoon est une famille de programmes malveillants très destructrice qui efface efficacement les données de la machine qui en est victime. Un groupe connu sous le nom de « Cutting Sword of Justice » (« Épée tranchante de la justice ») s'est attribué le mérite de l'attaque de Saudi Aramco en publiant un message Pastebin le jour de l'attaque (en 2012) et a défini son action comme un acte contre la monarchie saoudienne.

2017 a été une année difficile en matière d'attaques destructrices. Elles continueront d'augmenter, tirant parti de leur statut de type de cyberattaque le plus visible.

Les attaques de Shamoon 2.0 en novembre 2016 avaient ciblé des organisations de différents secteurs stratégiques et économiques d'Arabie Saoudite. Tout comme la version précédente, le wiper Shamoon 2.0 a pour objectif la destruction massive de systèmes à l'intérieur d'organisations compromises. Lors de son enquête sur les attaques de Shamoon 2.0, Kaspersky Lab a également découvert un programme malveillant de type wiper jusqu'alors inconnu, qui semble cibler des organisations en Arabie Saoudite. Nous avons appelé ce nouveau wiper StoneDrill et sommes presque certains qu'il est lié au groupe de menaces persistantes sophistiquées Newsbeef.

En plus de StoneDrill et Shamoon, 2017 a été une année difficile en matière d'attaques destructrices. L'attaque ExPetr/NotPetya, qui avait été initialement classée dans la catégorie des ransomwares, s'est avérée être elle aussi le fait d'un wiper habilement camouflé. ExPetr a été suivie par d'autres vagues d'attaques de « ransomwares », qui laissent peu de chances aux victimes de récupérer leurs données. Toutes ces attaques de wipers ont été savamment masquées derrière une apparence de ransomware. On a peut-être moins entendu parler de la vague d'attaques de « wipers déguisés en ransomwares » observée en 2016, qui provient de la menace persistante sophistiquée CloudAtlas contre des établissements financiers en Russie.

En 2018, nous estimons que les attaques destructrices continueront d'augmenter, tirant parti de leur statut de type de cyberattaque le plus visible.

Davantage de subversion de la cryptographie

En mars 2017, les propositions de plans de chiffrement IoT (« Internet of Things », Internet des objets) élaborées par la NSA (National Security Agency, agence américaine de la sécurité) ont été remises en question avec le retrait et le second report des approbations concernant les normes ISO Simon et Speck.

En août 2016, Juniper Networks a annoncé la découverte de deux mystérieux backdoors dans leurs pare-feu NetScreen. Le plus intéressant des deux était peut-être un changement extrêmement subtil de constantes utilisées pour le générateur de nombres aléatoires Dual_EC, qui permettrait à un attaquant bien informé de décrypter le trafic VPN des appareils NetScreen. L'algorithme Dual_EC original a été conçu par la NSA et mis en place par le NIST (National Institute of Standards and Technology, institut américain des normes et technologies). En 2013, un rapport de Reuters a suggéré que la NSA avait payé 10 millions de dollars à RSA pour introduire l'algorithme vulnérable dans ses produits afin de saboter le chiffrement. Même si la possibilité théorique d'un backdoor a été identifiée dès 2007, plusieurs entreprises (y compris Juniper) ont continué de l'utiliser avec un ensemble de constantes différent, ce qui le sécuriserait, en théorie. Il semble que cette différence d'ensemble de constantes ait suffisamment contrarié certains auteurs de menaces persistantes sophistiquées pour qu'ils piratent Juniper et changent les constantes au profit d'un ensemble qu'ils pouvaient contrôler et exploiter pour décrypter les connexions VPN.

En 2018, des failles cryptographiques plus graves seront découvertes et corrigées, que cela se fasse via des normes ou des implémentations spécifiques.

Ces tentatives ne sont pas passées inaperçues. En septembre 2017, un groupe international d'experts en cryptographie a forcé la NSA à abandonner deux nouveaux algorithmes de chiffrement que l'organisation espérait voir normaliser.

En octobre 2017, on a appris l'existence d'une faille dans une bibliothèque cryptographique utilisée par Infineon dans ses puces matérielles pour la génération de nombres premiers RSA. Alors que la faille semble avoir été involontaire, cela pose la question du degré de sécurité des technologies de chiffrement sous-jacentes utilisées dans notre vie quotidienne, qu'il s'agisse de cartes à puce, de réseaux Wi-Fi ou de trafic Web crypté. En 2018, nous prévoyons que des failles cryptographiques plus graves seront découvertes et (espérons-le) corrigées, que cela se fasse via des normes ou des implémentations spécifiques.

Début de crise au sujet de l'identification dans l'e-commerce

Ces dernières années ont été ponctuées par des violations à grande échelle de plus en plus catastrophiques des informations d'identification personnelle. Le dernier exemple en date est la violation Equifax qui aurait affecté 145,5 millions d'Américains. Si nombreux sont ceux qui sont devenus insensibles à la gravité de ces violations, il est important de comprendre que la divulgation d'informations d'identification personnelle à grande échelle met en danger un pilier fondamental de l'e-commerce et les avantages administratifs de l'utilisation d'Internet pour les documents importants. Bien sûr, la fraude et le vol d'identité sont un problème depuis longtemps, mais que se passe-t-il lorsque les informations d'identification fondamentales sont si largement répandues qu'elles ne sont tout simplement pas fiables du tout ? Le commerce et les institutions gouvernementales (notamment aux États-Unis) devront choisir entre revenir sur le confort moderne offert par Internet pour les opérations, ou mettre les bouchées doubles sur l'adoption d'autres solutions multi-facteur. Peut-être que des alternatives jusqu'ici résistantes comme ApplePay deviendront populaires pour garantir l'identification et les transactions, mais en attendant, nous pourrions voir un ralentissement de l'évolution d'Internet comme moyen crucial pour moderniser les processus administratifs fastidieux et réduire les coûts d'exploitation.

Davantage de piratages de routeurs et de modems

Les routeurs et modems, d'une importance critique pour les opérations quotidiennes, ont tendance à exécuter des logiciels propriétaires qui ne sont ni corrigés, ni surveillés.

Les routeurs et modems représentent un autre facteur connu de vulnérabilité jusqu'ici largement ignoré. Présents aussi bien dans les foyers que dans les entreprises, ces éléments matériels sont partout, sont d'une importance critique pour les opérations quotidiennes et ont tendance à exécuter des logiciels propriétaires qui ne sont ni corrigés, ni surveillés. De plus, ces petits ordinateurs sont par essence en contact direct avec Internet et se trouvent donc à un point crucial pour un attaquant cherchant à accéder à un réseau de façon persistante et sans être remarqué. En outre, comme de très bonnes recherches récentes l'ont montré, dans certains cas, les attaquants pourraient même être en mesure d'usurper l'identité de différents internautes, ce qui permettrait de détourner la piste d'un attaquant vers une adresse de connexion différente. On ne peut pas l'ignorer quand on sait que l'intérêt croît pour les détournements et les fausses bannières. Un examen plus minutieux de ces appareils donnera inévitablement lieu à des constatations intéressantes.

Vers le chaos social

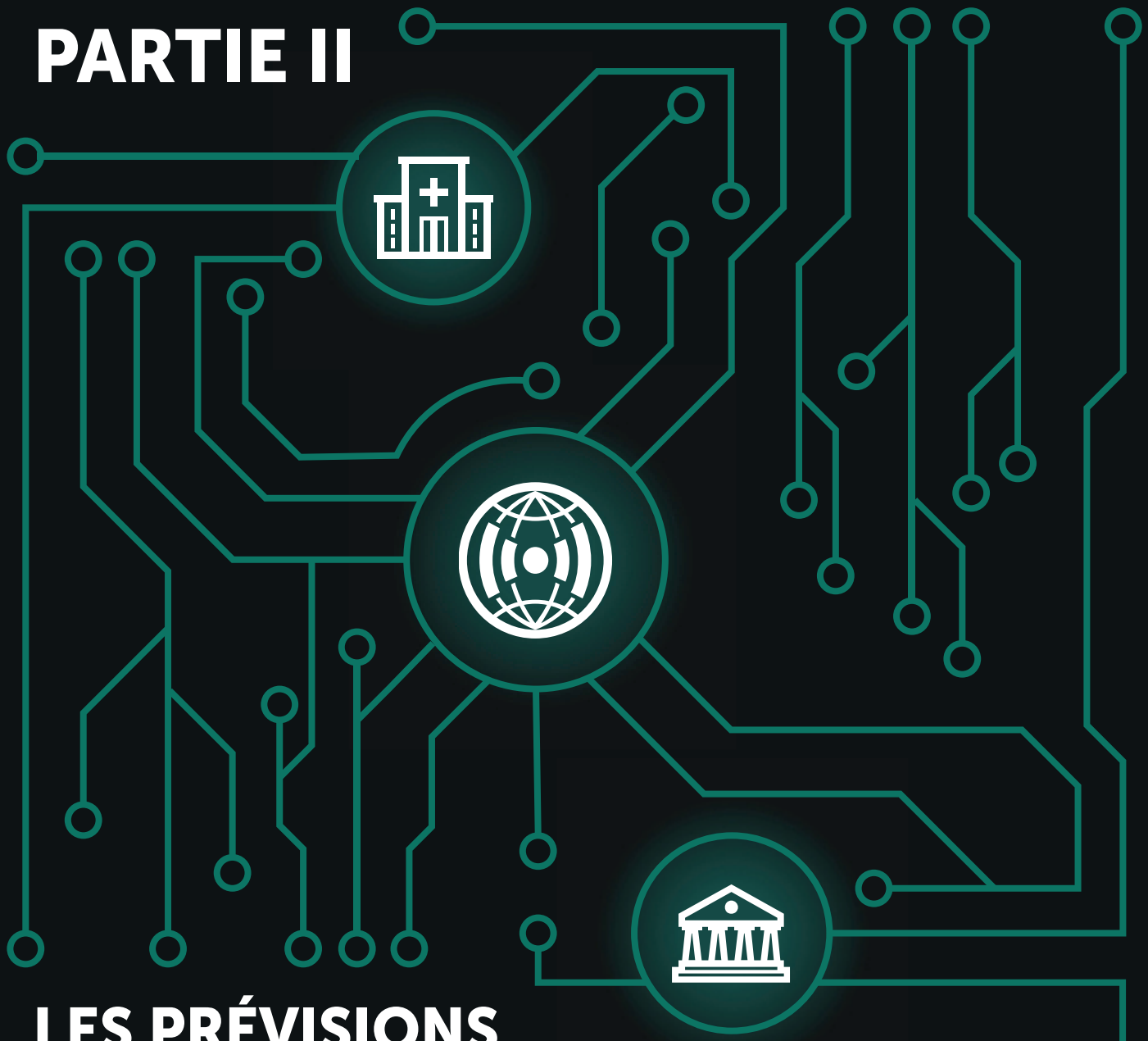
L'année écoulée a été témoin d'un regain d'intérêt pour la guerre de l'information et, au-delà des fuites et des scandales politiques, les réseaux sociaux eux-mêmes ont pris un rôle politisé qui a dépassé toutes nos attentes. Que ce soit en raison des commentaires d'experts politiques ou des piques humoristiques mais déroutantes des auteurs de South Park envers le PDG de Facebook, les regards se sont tournés vers différents géants des réseaux sociaux qui exigent un certain niveau de vérification et l'identification des faux utilisateurs et des robots qui essaient d'exercer des niveaux d'influence sociale disproportionnés. Malheureusement, il est devenu évident que ces réseaux (qui fondent leur succès sur des métriques quantifiées comme le nombre d'utilisateurs actifs journalier) sont peu enclins à purger leur base d'utilisateurs des robots. Même lorsque ces robots ont un objectif évident ou peuvent être suivis et tracés par des chercheurs indépendants. Nous nous attendons à ce qu'avec la persistance des abus manifestes et l'accès des grands réseaux de robots à de plus grandes masses de personnes politiquement détestables, le retour de flamme principal soit dirigé vers l'utilisation des réseaux sociaux eux-mêmes, et à ce que les utilisateurs dégoûtés recherchent des alternatives aux géants populaires qui se complaisent dans les avantages des usages abusifs générateurs de bénéfices et de clics.

CONCLUSION

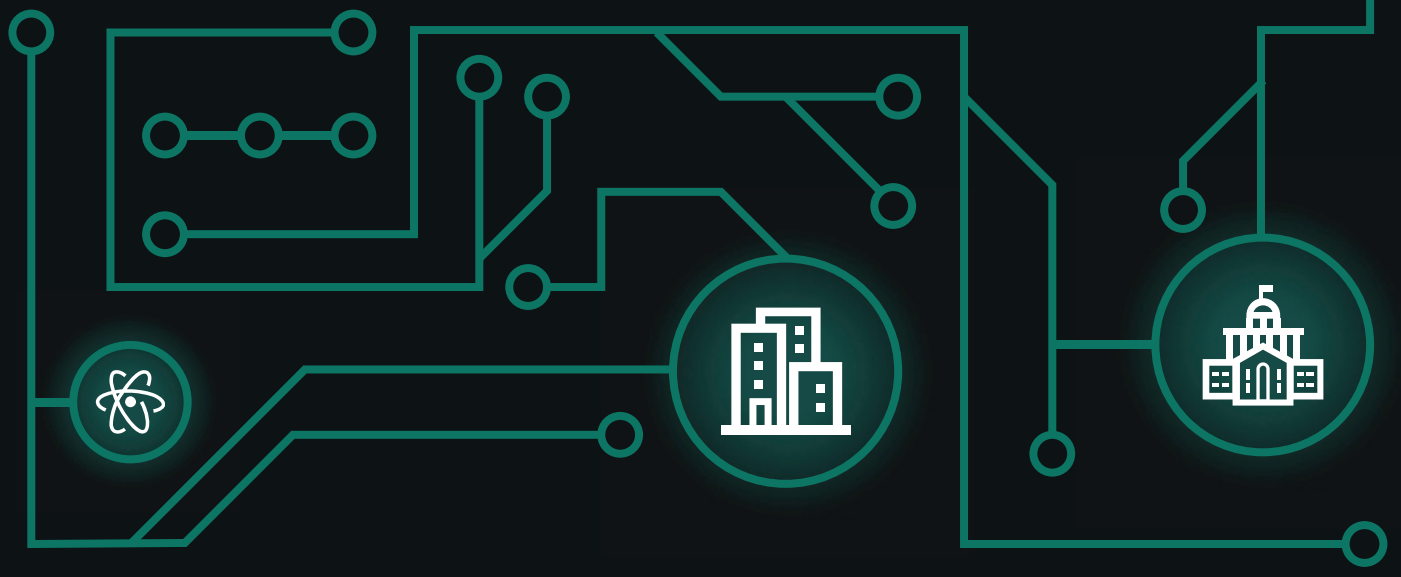
En 2017, nous avons annoncé la mort des indicateurs de compromission. En 2018, nous nous attendons à voir des cybercriminels sophistiqués utiliser leurs nouvelles forces, affûter leurs nouveaux outils et affiner les angles d'attaque terrifiants décrits ci-dessus. Les thèmes et les tendances de chaque année ne doivent pas être considérés isolément : ils s'appuient les uns sur les autres pour enrichir un paysage de menace en croissance constante, des menaces auxquelles sont confrontés les utilisateurs de tous types, qu'il s'agisse des particuliers, des entreprises ou des gouvernements. Le seul sursis constant à ces assauts est le partage et l'application éclairée d'une threat intelligence de qualité.

Bien que ces prévisions couvrent les tendances en matière de menaces ciblées avancées, chaque secteur industriel fera face à ses propres défis. En 2018, nous avons voulu mettre l'accent sur certains d'entre eux.

PARTIE II

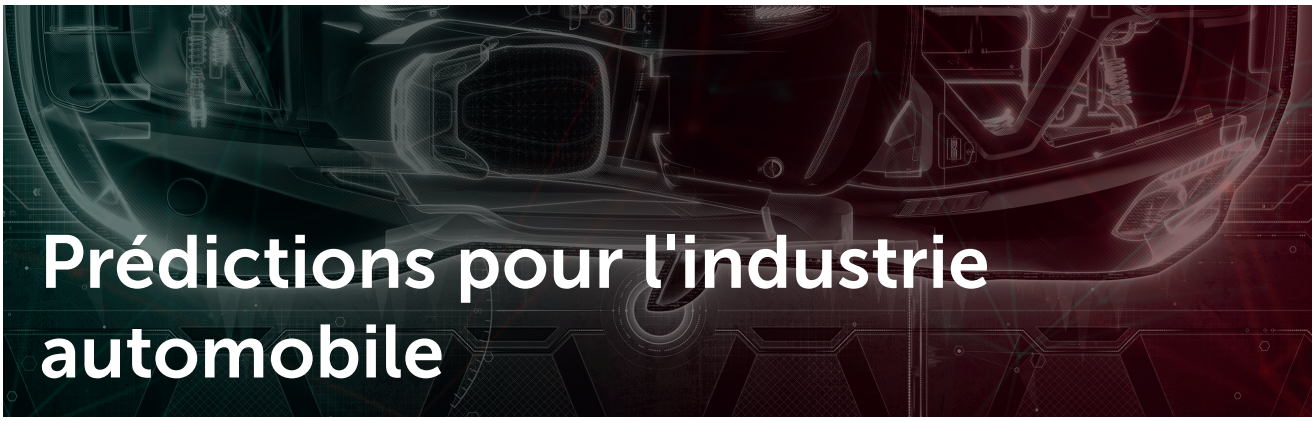


LES PRÉVISIONS POUR DIFFÉRENTS SECTEURS INDUSTRIELS ET TECHNOLOGIQUES



INTRODUCTION

Nous vivons dans un monde connecté où les technologies numériques sont devenues partie intégrante de la vie quotidienne des particuliers et des organisations. De nouvelles vulnérabilités et menaces ont vu le jour. Certains secteurs de l'industrie font actuellement l'objet de plus de cyberattaques que d'autres. Dans cette section de prévisions pour l'industrie et la technologie, nous avons choisi de présenter pour quelques-uns de ces secteurs certains des principaux risques qui pourraient se profiler, ainsi que leur impact potentiel.



Prédictions pour l'industrie automobile

LA SITUATION EN 2017

Les voitures modernes ne sont plus simplement des véhicules électro-mécaniques. À chaque génération, elles deviennent de plus en plus connectées et intègrent davantage de technologies intelligentes, qui les rendent plus astucieuses, efficaces, confortables et sûres. Le marché de l'automobile connectée augmente à un taux de croissance annuel composé de 45 % sur cinq ans, soit 10 fois plus vite que le marché de l'automobile dans son ensemble.

Le marché de l'automobile connectée augmente à un taux de croissance annuel composé de 45 % sur cinq ans, soit 10 fois plus vite que le marché de l'automobile dans son ensemble.

Dans certaines zones (par ex. l'UE ou la Russie), les systèmes connectés à deux voies (eCall, ERA-GLONASS) sont couramment mis en œuvre à des fins de sécurité et de surveillance ; et tous les principaux fabricants automobiles offrent désormais des services qui permettent aux utilisateurs d'interagir à distance avec leur voiture via une interface Web ou une application mobile.

Les diagnostics à distance, la télématique et l'infodivertissement connecté améliorent considérablement la sécurité et le plaisir du conducteur, mais présentent également de nouveaux défis pour le secteur de l'automobile puisqu'ils transforment les véhicules en cibles de premier ordre pour les cyberattaques. Le risque croissant d'infiltration des systèmes de véhicules ou de violation de leur sécurité et de leurs données privées et financières oblige les fabricants à comprendre et à mettre en œuvre la sécurité informatique. Ces dernières années ont vu un certain nombre d'exemples (ici, ici, et là) qui ont mis en lumière la vulnérabilité des voitures connectées.

LA SITUATION PRÉVUE EN 2018

Gartner estime qu'il y aura un quart de milliard de voitures connectées sur les routes d'ici 2020. D'autres suggèrent que d'ici là, environ 98 % des voitures seront connectées à Internet. Les menaces auxquelles nous faisons face maintenant, et celles que nous nous attendons à devoir affronter au cours de l'année à venir, ne devraient pas être considérées séparément ; elles font partie d'un continuum. Plus il y a de véhicules connectés et plus ils sont connectés de différentes manières, plus la surface et les possibilités d'attaque sont importantes.

Voici quelques-unes des menaces qui pèseront sur le secteur de l'automobile au cours des 12 prochains mois :

Des vulnérabilités introduites par le manque d'attention ou d'expertise du fabricant, combinées à des pressions concurrentielles. La gamme de services de mobilité connectés disponibles va continuer d'augmenter, tout comme le nombre d'acteurs qui les développent et les fournissent. Cette offre toujours plus étendue (et la probabilité que les produits/fournisseurs soient de qualité variable), conjuguée à un marché férocement concurrentiel, pourrait mener à des raccourcis ou à des failles en matière de sécurité qui constituent une porte ouverte pour les pirates.

Des vulnérabilités introduites par la complexité croissante des produits et services. Les fabricants du secteur de l'automobile se concentrent de plus en plus sur la prestation de services interconnectés multiples. Chaque lien constitue un point faible potentiel que les attaquants saisiront sans se faire prier. Un attaquant a juste besoin de trouver un point vulnérable, qu'il s'agisse par exemple d'un périphérique tel que le Bluetooth pour téléphone ou d'un système de téléchargement de musique. À partir de là, il peut prendre le contrôle des composants électriques essentiels à la sécurité comme les freins ou le moteur, et faire des ravages.

Aucun code de logiciel n'est totalement dépourvu de bugs, et qui dit bugs, dit vulnérabilités potentielles. Les véhicules comportent déjà plus de 100 millions de lignes de code. Cela représente en soi une surface d'attaque massive pour les cybercriminels. Et comme de plus en plus d'éléments connectés sont installés dans les véhicules, le volume du code va monter en flèche, augmentant le risque d'erreurs. Certains fabricants automobiles, notamment Tesla, ont introduit des programmes de « bug bounty » pour faire face à ce problème.

De plus, sachant que les logiciels sont écrits par différents développeurs, installés par différents fournisseurs, et envoient souvent leurs rapports à différentes plateformes de gestion, aucun acteur n'aura de visibilité, et encore moins de contrôle, sur l'ensemble du code source d'un véhicule. Cela pourrait aider les attaquants à ne pas être détectés.

Les applications sont du pain bénit pour les cybercriminels. Il existe un nombre croissant d'applications pour smartphone, dont bon nombre sont publiées par des constructeurs automobiles, que les propriétaires peuvent télécharger pour déverrouiller leur voiture à distance, vérifier l'état du moteur ou trouver leur véhicule. Les chercheurs ont déjà démontré comment ces applications pouvaient être piratées. Il ne faudra pas longtemps avant que des applications à chevaux de Troie apparaissent et injectent des programmes malveillants au cœur du véhicule de la victime sans qu'elle ne se doute de rien.

Au vu de la multiplication des composants connectés introduits par des entreprises plus familières avec le matériel que les logiciels, il existe un risque croissant de négligence de la nécessité de mises à jour constantes. Cela pourrait rendre plus difficile, voire impossible, la correction à distance des problèmes connus. Les rappels de véhicules prennent du temps et coûtent de l'argent et, pendant ce temps, de nombreux conducteurs seront sans protection.

Les véhicules connectés engendreront et traiteront toujours plus de données sur eux-mêmes, mais aussi sur les trajets et même des données personnelles sur les occupants. Les attaquants qui cherchent à vendre des données sur le marché noir ou à les utiliser pour extorquer de l'argent ou exercer un chantage vont de plus en plus s'y intéresser. Les constructeurs automobiles sont déjà sollicités par des sociétés de marketing avides d'obtenir un accès légitime aux données des passagers et des trajets pour proposer des publicités en temps réel selon l'emplacement du véhicule.

Heureusement, la sensibilisation et la compréhension croissantes des menaces de sécurité entraîneront l'apparition sur le marché des premiers appareils de cybersécurité pour effectuer des diagnostics à distance et recueillir des données télématiques.

En outre, les législateurs mettront en place des exigences et des recommandations pour rendre la cybersécurité obligatoire pour tous les véhicules connectés.

Dernier point, mais non des moindres, en plus des certifications de sécurité existantes, de nouvelles organisations responsables de la certification en cybersécurité seront créées. Elles utiliseront des normes clairement définies pour évaluer les véhicules connectés en fonction de leur résistance aux cyberattaques.

Actions recommandées

Pour faire face à ces risques, il faut faire de la sécurité une norme dès la conception et l'axer sur différentes parties de l'écosystème de la voiture connectée. Des solutions logicielles défensives pourraient être installées localement sur certains composants électriques (les freins par exemple) pour renforcer leur protection contre les attaques. Par ailleurs, des logiciels peuvent protéger le réseau interne du véhicule dans son ensemble, en examinant toutes les communications réseau, en signalant tout changement dans les comportements standards du réseau interne au véhicule et en empêchant les attaques d'avancer dans le réseau. D'une manière générale, une solution doit protéger tous les composants connectés à l'extérieur, via Internet. Les services de sécurité Cloud peuvent détecter et corriger les menaces avant qu'elles n'atteignent le véhicule. Ils peuvent également envoyer au véhicule des mises à jour « over-the-air » et des renseignements en temps réel. Tout ceci devra s'appuyer sur des normes industrielles rigoureuses et cohérentes.

Prévisions pour le secteur de la santé connectée

LA SITUATION EN 2017

Nous avons trouvé un accès ouvert à environ 1 500 appareils d'imagerie médicale.

En 2017, des recherches Kaspersky Lab ont révélé à quel point les renseignements médicaux et les données des patients stockés au sein des infrastructures de santé connectées étaient laissés sans protection et accessibles en ligne à tout cybercriminel motivé. Par exemple, nous avons trouvé un accès ouvert à environ 1 500 appareils d'imagerie médicale. En outre, nous avons constaté qu'une quantité importante de logiciels médicaux connectés et d'applications Web contenaient des vulnérabilités, dont certaines étaient publiques.

Ce risque est accru parce que les cybercriminels sont de plus en plus conscients de la valeur des informations de santé, de leur disponibilité et de la volonté des établissements de santé de payer pour les récupérer.

LA SITUATION PRÉVUE EN 2018

Les menaces qui pèsent sur le secteur de la santé se multiplieront à mesure qu'augmentera le déploiement d'appareils connectés et d'applications Web vulnérables par les établissements de santé.

Les menaces qui pèsent sur le secteur de la santé se multiplieront à mesure qu'augmentera le déploiement d'appareils connectés et d'applications Web vulnérables par les établissements de santé. Les soins de santé connectés ont différentes motivations, parmi lesquelles le besoin d'optimiser les ressources et les coûts, celui de travailler de plus en plus à distance, le besoin en soins à domicile des personnes atteintes de maladies chroniques comme le diabète et des personnes âgées, l'envie des consommateurs d'avoir un mode de vie sain et la reconnaissance du fait que le partage de données et le monitoring des patients entre les organisations peuvent considérablement améliorer la qualité et l'efficacité des soins médicaux.

Voici quelques-unes des menaces qui pèseront sur ces tendances au cours des 12 prochains mois :

Nous verrons une augmentation des attaques visant l'équipement médical avec pour objectif l'extorsion d'argent, des interruptions malveillantes, voire pire. Le volume d'équipement médical spécialisé connecté à des réseaux informatiques est en hausse. Un grand nombre de ces réseaux sont privés, mais une connexion Internet externe peut être suffisante pour que les agresseurs s'introduisent et diffusent leurs programmes malveillants via le réseau « fermé ». Cibler l'équipement peut perturber les soins et se révéler fatal, de sorte que la probabilité que l'établissement médical paie est très élevée.

Il y aura également une augmentation du nombre d'attaques ciblées axées sur le vol de données. La quantité de renseignements médicaux et de données de patients conservés et traités par les systèmes de santé connectés s'accroît de jour en jour. Ces données sont extrêmement précieuses sur le marché noir et peuvent également être utilisées pour extorquer de l'argent et faire du chantage. Les criminels ne sont pas les seuls à pouvoir être intéressés : l'employeur ou la compagnie d'assurance de la victime pourrait vouloir ces informations car elles pourraient avoir un impact sur ses primes ou même sur la sécurité de son emploi.

Il y aura plus d'incidents liés à des attaques de ransomwares contre des établissements de santé. Il s'agira de chiffrement des données ainsi que de blocage d'appareils : l'équipement médical connecté est souvent coûteux et parfois essentiel à la vie de certains patients, ce qui fait d'eux une cible de premier ordre pour les attaques et l'extorsion.

Le concept de périmètre d'entreprise clairement défini continuera de reculer dans les établissements médicaux. Les stations de travail, serveurs, appareils mobiles et équipements sont de plus en plus souvent connectés. Cela donnera aux criminels davantage de possibilités d'accéder aux informations et réseaux médicaux. Maintenir la sécurité des défenses et des terminaux sera un défi toujours plus grand pour les équipes de sécurité dans le domaine de la santé, car chaque nouvel appareil représentera un nouveau point d'entrée dans l'infrastructure de l'établissement.

Les professionnels de la santé et les données sensibles et confidentielles transmises entre « objets portables » connectés, comme les implants, seront de plus en plus la cible d'attaques à mesure que l'utilisation de tels appareils pour le diagnostic, le traitement et les soins préventifs médicaux continuera d'augmenter. Les stimulateurs cardiaques et les pompes à insuline en sont de parfaits exemples.

Les systèmes d'information de santé nationaux et régionaux qui partagent avec les praticiens, hôpitaux, cliniques et autres installations locales des données de patients dont la sécurité laisse à désirer, par exemple parce qu'elles ne sont pas codées, seront de plus en plus ciblés par les attaquants qui cherchent à intercepter des données échappant à la protection des pare-feu d'entreprise. Il en sera de même pour les données partagées entre les installations médicales et les sociétés d'assurance-maladie.

L'utilisation croissante par les consommateurs de gadgets connectés sur leur santé et condition physique permettra aux attaquants d'accéder à un volume considérable de données à caractère personnel qui sont généralement peu protégées. Avec la popularité des modes de vie connectés et sains, les bracelets et moniteurs d'activité physique, montres intelligentes, etc., transporteront et transmettront des quantités toujours plus importantes de données personnelles avec rien de plus qu'une sécurité de base, et les cybercriminels n'hésiteront pas à les exploiter.

Les attaques perturbatrices, qu'il s'agisse d'attaques par déni de service ou via un ransomware qui détruit tout simplement des données (comme WannaCry), sont une menace croissante pour les établissements de santé qui misent de plus en plus sur le numérique. Les stations de travail toujours plus nombreuses, la gestion électronique des dossiers et les processus commerciaux numériques qui sous-tendent toute organisation moderne élargissent la surface d'attaque pour les cybercriminels. Dans le domaine de la santé, ils sont couplés à un facteur « urgence », puisque toute perturbation peut réellement devenir une question de vie ou de mort.

Dernier point, mais pas des moindres, les technologies émergentes telles que les membres artificiels connectés, les prothèses pour améliorations physiologiques intelligentes, la réalité augmentée intégrée, etc., conçues à la fois pour répondre à une déficience et créer de meilleurs êtres humains, plus forts et en meilleure forme, offriront aux attaquants de nouvelles possibilités d'actions malveillantes et de préjudices à moins que la sécurité y soit intégrée dès les premiers instants de leur conception.

Prévisions pour les services financiers et la fraude

LA SITUATION EN 2017

Les données de clients sont un outil clé pour les attaques frauduleuses à grande échelle.

En 2017, les attaques frauduleuses dans le domaine des services financiers se sont de plus en plus centrées sur les comptes. Les données de clients sont un outil clé pour les attaques frauduleuses à grande échelle et les violations de données particulièrement fréquentes ont fourni aux cybercriminels de précieuses sources de renseignements personnels à utiliser pour les attaques basées sur le piratage de compte ou sur une fausse identité. Ces attaques centrées sur les comptes peuvent entraîner de nombreuses autres pertes, les clients n'étant notamment plus prêts à accorder leur confiance et à confier leurs données. Ainsi, l'atténuation des menaces est plus importante que jamais pour les entreprises et les clients de services financiers.

LA SITUATION PRÉVUE EN 2018

2018 sera une année d'innovation dans le secteur des services financiers, car le rythme d'évolution continue d'accélérer dans ce domaine. Comme davantage de canaux et d'offres de services financiers émergent, les menaces vont se diversifier. Les services financiers devront mettre l'accent sur la prévention de la fraude omnicanal pour identifier avec succès plus de fraudes allant des comptes en ligne à de nouveaux canaux. Les derniers types de paiement à succès seront de plus en plus la cible de tentatives d'attaques alors que leur rentabilité augmentera aux yeux des attaquants.

2018 sera une année d'innovation dans le secteur des services financiers, car le rythme d'évolution continue d'accélérer dans ce domaine.

Les défis du paiement en temps réel

La demande croissante des consommateurs en transactions financières en temps réel et transfrontalières fait naître une pression pour analyser les risques plus rapidement. Les attentes des consommateurs en matière de fluidité des paiements rendent cette tâche encore plus difficile. Les services financiers devront repenser les processus d'identification des clients pour les rendre plus efficaces. Le machine learning et éventuellement des solutions basées sur l'intelligence artificielle seront aussi essentiels pour répondre au besoin d'accélérer la détection du risque et de la fraude.

Piratage informatique

Les services financiers devront rester concentrés sur les techniques d'attaques qui ont fait leurs preuves. En dépit de menaces émergentes plus sophistiquées, le piratage informatique et le phishing constituent toujours des attaques parmi les plus simples et les plus rentables : exploiter ce maillon faible qu'est l'élément humain. Les informations aux clients et la formation des salariés devraient continuer d'améliorer la sensibilisation aux attaques et escroqueries les plus récentes.

Menaces mobiles

Selon le dernier indice de cybersécurité Kaspersky Lab, de plus en plus d'activités en ligne ont désormais lieu sur appareil mobile. Par exemple, 35 % des personnes utilisent à présent leur smartphone pour les services bancaires en ligne et 29 % pour les systèmes de paiement en ligne (l'année précédente, ces pourcentages n'atteignaient que 22 % et 19 % respectivement). Ces consommateurs qui privilégient les appareils mobiles seront de plus en plus souvent des cibles de choix pour les fraudes. Les cybercriminels utiliseront des familles de programmes malveillants qui ont fait leurs preuves et d'autres plus récentes pour voler les informations bancaires des utilisateurs de manière créative. En 2017, nous avons constaté la modification de la famille de programmes malveillants Svpeng. En 2018, d'autres familles d'attaques contre les appareils mobiles feront à nouveau surface pour cibler les identifiants bancaires à l'aide de nouvelles fonctionnalités. L'identification et la suppression des programmes malveillants mobiles sont essentielles si les établissements de services financiers veulent tuer les attaques dans l'œuf.

Par exemple, 35 % des personnes utilisent à présent leur smartphone pour les services bancaires en ligne et 29 % pour les systèmes de paiement en ligne.

Violation de données

Les violations de données continueront de faire la une en 2018 et l'impact secondaire sur les établissements financiers se fera sentir par le biais de faux comptes piégés et de piratages de compte. Les violations de données, bien que plus difficiles à commettre que les fraudes individuelles contre les clients, sont très intéressantes pour les criminels du fait du volume élevé de données de clients exposées en une fois. Les services financiers doivent tester leurs défenses de manière régulière et utiliser des solutions afin de détecter tout accès suspect dès les premières étapes.

Cibles dans le domaine des cryptomonnaies

Davantage d'établissements financiers étudieront l'utilisation de cryptomonnaies, ce qui fera de ces monnaies des cibles cruciales pour les attaques de cybercriminels. Nous avons déjà vu que les exemples de programmes malveillants de minage étaient en augmentation en 2017, et davantage de tentatives d'exploitation de ces monnaies auront lieu en 2018. Il faudrait utiliser des solutions capables de détecter les familles de programmes malveillants les plus récentes, ainsi qu'intégrer aux stratégies de prévention la dernière threat intelligence. [Voir nos Prévisions de menaces pour les cryptomonnaies pour de plus amples informations à ce sujet.]

Piratage de compte

L'augmentation des paiements physiques sécurisés grâce à des puces et d'autres améliorations des points de vente a eu pour résultat une relocalisation de la fraude en ligne au cours de la dernière décennie. À présent, alors que la sécurité des paiements en ligne s'améliore, notamment grâce à la tokenisation et les technologies biométriques, les fraudeurs passent au piratage de comptes. Les estimations du secteur suggèrent que ce genre de fraude coûtera des milliards de dollars si les fraudeurs continuent d'exploiter ce vecteur d'attaque très rentable. Les services financiers devront repenser les identifications numériques et utiliser des solutions novatrices pour s'assurer que chaque client est bien la personne qu'il prétend être, à chaque fois.

La pression de l'innovation

De plus en plus d'entreprises s'aventureront dans le monde des solutions de paiement et de l'Open Banking en 2018. L'innovation sera cruciale pour les entreprises de services financiers existantes à la recherche d'un avantage concurrentiel par rapport à un nombre croissant de concurrents. Comprendre les complications réglementaires peut déjà être assez difficile, sans parler d'évaluer le risque d'attaque sur de nouveaux canaux. Ces nouvelles offres seront dès leur sortie les cibles des fraudeurs et toute nouvelle solution qui ne sera pas fondée sur la sécurité s'avérera être une cible facile pour les cybercriminels.

La fraude en tant que service

Avec la communication internationale clandestine entre cybercriminels, les connaissances sont partagées rapidement et les attaques peuvent se propager dans le monde encore plus vite. Des services de fraude sont offerts sur le Dark Web, qu'il s'agisse de bots, de services de traduction de phishing ou d'outils d'accès à distance. Les cybercriminels moins expérimentés achètent et utilisent ces outils, ce qui implique plus de tentatives d'attaques à bloquer pour les services financiers. Le partage des connaissances entre les services ainsi que le recours à des services de threat intelligence seront essentiels dans l'atténuation de ces menaces.

Attaques de guichets automatiques

Les guichets automatiques continueront d'attirer l'attention de nombreux cybercriminels. En 2017, les chercheurs de Kaspersky Lab ont découvert, entre autres, des attaques sur les systèmes de distributeurs qui utilisaient de nouveaux programmes malveillants, des opérations distantes et sans fichier, et un programme malveillant ciblant les guichets automatiques appelé Cutlet Maker, qui était vendu ouvertement sur le marché du DarkNet pour quelques milliers de dollars avec un guide de d'utilisation étape par étape. Kaspersky Lab a publié un rapport sur les futurs scénarios d'attaque de distributeurs ciblant les systèmes d'authentification de ces appareils.

Prévisions pour la sécurité industrielle

LA SITUATION EN 2017

La menace la plus importante pour les systèmes industriels en 2017 a été le ransomware de chiffrement.

2017 a été l'une des années les plus intenses en matière d'incidents touchant la sécurité des informations des systèmes industriels. Les chercheurs en sécurité ont découvert des centaines de nouvelles vulnérabilités, recherché de nouveaux vecteurs de menace ciblant les systèmes de contrôle industriel (SCI) et les procédés industriels, recueilli et analysé les statistiques sur les infections accidentelles des systèmes industriels et détecté des attaques ciblées sur les entreprises industrielles (plus précisément, Shamoon 2.0/StoneDrill). Et, pour la première fois depuis Stuxnet, ils ont découvert et analysé un ensemble d'outils malveillants ciblant les systèmes physiques : CrashOverride/Industroyer, que certains experts ont décrit comme une « cyberarme ».

Toutefois, la menace la plus importante pour les systèmes industriels en 2017 a été le ransomware de chiffrement. Selon Kaspersky Lab ICS CERT, dans la première moitié de l'année, les systèmes d'information industriels dans 63 pays à travers le monde ont fait l'objet de nombreuses attaques impliquant des ransomwares de chiffrement appartenant à 33 familles différentes. Les attaques destructrices des ransomwares WannaCry et ExPetr semblent avoir changé à jamais l'attitude des entreprises industrielles face au problème de la protection des systèmes de production essentiels.

LA SITUATION PRÉVUE EN 2018

Une montée des infections générales et accidentelles par programmes malveillants

À quelques exceptions près, les groupes cybercriminels n'ont pas encore découvert de technique simple et fiable pour rentabiliser les attaques sur les systèmes d'information industriels. Nous verrons toujours en 2018 des infections accidentelles et des incidents sur les réseaux industriels causés par le code malveillant « normal » (général) visant les cibles plus traditionnelles des cybercriminels, notamment les réseaux d'entreprise. Dans le même temps, nous constaterons probablement que ces situations auront des conséquences plus graves pour les environnements industriels. La mise à jour régulière des logiciels dans les systèmes industriels et les réseaux d'entreprise demeurera problématique, malgré les avertissements répétés des spécialistes de la sécurité.

Un risque accru d'attaques de ransomwares ciblées

Les attaques ExPetr et WannaCry ont appris aux experts en sécurité et aux cybercriminels que les systèmes de technologie opérationnelle (OT, « operational technology ») pouvaient être encore plus vulnérables à de telles attaques que les systèmes informatiques, et étaient également accessibles via Internet. En outre, les dégâts causés par les programmes malveillants dans le réseau OT pouvaient être plus importants que dans le réseau d'entreprise correspondant, et dans le cas de l'OT, les combattre « dans le feu de l'action » est beaucoup plus difficile. Les entreprises industrielles ont démontré à quel point leur personnel pouvait être inefficace et mal organisé en cas de cyberattaque sur leur infrastructure OT. Tous ces facteurs font des systèmes industriels une cible alléchante pour les attaques par ransomwares.

Davantage d'incidents de cyberespionnage industriel

La menace croissante des attaques par ransomwares organisées contre les entreprises industrielles pourrait déclencher le développement d'un domaine de cybercriminalité parent : le vol de données de systèmes d'information industriels et leur utilisation pour la préparation et la mise en œuvre d'attaques ciblées (notamment des attaques par ransomwares).

De nouveaux segments du marché souterrain axés sur les attaques ciblant les systèmes industriels

Au cours des dernières années, nous avons constaté une demande croissante sur le marché noir en vulnérabilités « zero-day » ciblant les SCI. Cela nous indique que les criminels travaillent sur des campagnes d'attaques ciblées. Nous nous attendons à ce que les cybercriminels investissent davantage ce domaine en 2018, ce qui est susceptible d'entraîner l'apparition de nouveaux segments axés sur les données de configuration des SCI et sur des informations d'identification SCI volées dans les entreprises industrielles et, éventuellement, des offres de botnets avec nœuds « industriels ». La conception et la mise en œuvre de cyberattaques sophistiquées ciblant des objets physiques et des systèmes exige une connaissance approfondie des SCI et des industries concernées. La demande en ce type d'expertise devrait être le moteur de la croissance de domaines tels que le « programme malveillant en tant que service », la « conception de vecteur d'attaque en tant que service », la « campagne d'attaque en tant que service » et d'autres services liés aux attaques sur les entreprises industrielles.

De nouveaux types de programmes et d'outils malveillants

Nous allons probablement voir de nouveaux programmes malveillants utilisés pour cibler des réseaux et des biens industriels, avec des caractéristiques telles que la discrétion et la capacité de rester inactif dans le réseau informatique afin d'éviter la détection, et de ne s'activer que dans l'infrastructure OT, moins sécurisée. Une autre possibilité est l'émergence de ransomwares ciblant des appareils et actifs physiques SCI (pompes, commutateurs, etc.) sur le terrain.

Modifications des réglementations nationales

En 2018, de nouvelles initiatives réglementaires sur les systèmes d'automatisation industriels entreront en vigueur dans certains pays. Entre autres conséquences, cela va forcer les entreprises qui possèdent des infrastructures critiques et des biens industriels critiques à faire plus d'effort dans leur évaluation de la cybersécurité. À la suite de cela, nous découvrirons probablement de nouvelles vulnérabilités identifiées dans les systèmes industriels. Des incidents dans des entreprises industrielles et des attaques auparavant inconnues nous seront également révélés.

Les criminels vont profiter des analyses de menace publiées par les chercheurs en sécurité

En 2017, les chercheurs ont été efficaces pour trouver et rendre public divers nouveaux vecteurs d'attaques sur les infrastructures et biens industriels, ainsi que pour effectuer une analyse profonde des ensembles d'outils malveillants trouvés. Tout cela est bon pour la sécurité des installations industrielles. Toutefois, les criminels pourraient également faire usage de cette information. Par exemple, des hacktivistes pourraient tirer parti de la divulgation de l'ensemble d'outils CrashOverride/Industroyer pour exécuter des attaques par déni de service sur les systèmes d'alimentation. Des criminels pourraient concevoir des ransomwares ciblés et même inventer des procédés de rentabilisation des pannes d'électricité. Le concept du ver d'API (automate programmable) pourrait inspirer les criminels à créer dans le monde réel des vers malveillants qui se propageraient d'un API à un autre, alors que d'autres pourraient essayer de mettre en œuvre des programmes malveillants en utilisant un des langages standards pour la programmation d'API. Il est même possible que certains cybercriminels tentent d'élaborer des programmes malveillants d'API opérant à un niveau bas sur la base d'une approche démontrée par les chercheurs en sécurité des informations. Ces deux dernières approches pourraient poser de graves problèmes aux développeurs de solutions de sécurité existantes.

Hausse de la disponibilité et de l'investissement dans la cyberassurance industrielle

L'assurance pour les risques de cyberincident devient une partie intégrante de la gestion des risques pour les entreprises industrielles. Jusqu'à récemment, les risques associés aux incidents de cybersécurité étaient exclus des contrats d'assurance ; en effet, les compagnies d'assurance les assimilaient aux attentats. Mais la situation est en train de changer, avec de nouvelles initiatives lancées à la fois par les sociétés de cybersécurité et par les principaux acteurs du secteur de l'assurance. En 2018, cela permettra d'augmenter le nombre d'audits/d'évaluations de sécurité de systèmes d'automatisation industriels, ainsi que le nombre d'incidents de cybersécurité enregistrés et examinés.

Prévisions pour les cryptomonnaies

LA SITUATION EN 2017

Au cours des huit premiers mois de 2017, les produits de Kaspersky Lab ont protégé 1,65 million d'utilisateurs contre les mineurs de cryptomonnaie malveillants. D'ici à la fin de l'année, nous nous attendons à ce que ce nombre dépasse les deux millions.

Aujourd'hui, la cryptomonnaie n'est plus réservée aux geeks et aux professionnels de l'informatique. Elle commence à affecter la vie quotidienne de tout un chacun, plus qu'on ne le pense. Dans le même temps, les cybercriminels la considèrent de plus en plus comme une cible intéressante. Certaines cybermenaces ont été héritées des paiements électroniques, comme la modification de l'adresse du portefeuille destinataire lors de la transaction ou le vol de porte-monnaie électronique, par exemple. Toutefois, les cryptomonnaies ont donné lieu à de nouveaux moyens de rentabiliser les activités malveillantes.

En 2017, la principale menace mondiale pour les utilisateurs a été les ransomwares : pour récupérer les fichiers et les données chiffrées par les attaquants, les victimes devaient payer une rançon en cryptomonnaie. Au cours des huit premiers mois de 2017, les produits de Kaspersky Lab ont protégé 1,65 million d'utilisateurs contre les mineurs de cryptomonnaie malveillants, et d'ici à la fin de l'année, nous nous attendons à ce que ce nombre dépasse les deux millions. En outre, en 2017, nous avons vu le retour des voleurs de Bitcoin après quelques années passées dans l'ombre.

LA SITUATION PRÉVUE EN 2018

2018 est susceptible d'être l'année des mineurs Web malveillants.

Avec l'augmentation constante du nombre, de l'adoption et de la valeur de marché des cryptomonnaies, ces dernières resteront non seulement une cible attrayante pour les cybercriminels, mais elles conduiront aussi à l'utilisation de techniques et d'outils plus avancés afin d'en créer plus. Les cybercriminels vont rapidement tourner leur attention vers les plans de monétisation les plus rentables. Par conséquent, 2018 est susceptible d'être l'année des mineurs Web malveillants.

Les attaques de ransomwares vont forcer les utilisateurs à acheter des cryptomonnaies

Les cybercriminels vont continuer d'exiger des rançons en cryptomonnaies car leur marché est non réglementé et presque anonyme : nul besoin de partager des données avec quiconque, personne ne va bloquer l'adresse, personne ne va vous surprendre, et il y a peu de chances d'être suivi. Dans le même temps, une plus grande simplification du processus de monétisation mènera à une plus grande diffusion des chiffreurs.

Des attaques ciblées avec des mineurs

Nous nous attendons au développement d'attaques ciblées sur des entreprises en vue d'installer des mineurs. Alors que les ransomwares représentent un revenu potentiel élevé mais unique, les mineurs se traduiront par des gains moins élevés mais durables. Nous verrons l'année prochaine si ce dernier type d'attaque prendra le pas sur les ransomwares.

Les mineurs seront toujours plus nombreux et variés

L'année prochaine, le minage continuera de se propager à travers le globe, attirant au passage davantage de personnes. La participation de nouveaux mineurs dépendra de leur capacité à avoir accès à une source stable et gratuite d'électricité. Ainsi, nous allons voir l'augmentation des « mineurs internes » : davantage de salariés d'organismes gouvernementaux commenceront à miner sur des ordinateurs appartenant au domaine public, et davantage de salariés d'entreprises manufacturières commenceront à utiliser les installations de leur entreprise.

Le minage sur navigateur Web

Le « web-mining » est une technique de minage de cryptomonnaie utilisée directement dans le navigateur avec un script spécial installé sur une page Web. Les attaquants ont déjà prouvé qu'il était facile de charger un script sur un site Web compromis et d'engager les ordinateurs des visiteurs dans une activité de minage, et par conséquent d'ajouter plus de pièces au porte-monnaie des criminels. L'année prochaine, le web-mining changera radicalement la nature d'Internet, ouvrant de nouvelles voies à la monétisation des sites Web. Il remplacera notamment la publicité : les sites Web proposeront de supprimer définitivement un script de minage si l'utilisateur s'abonne à des contenus payants. Par ailleurs, différents types de divertissement, tels que des films, seront proposés gratuitement en échange de votre minage. Il en ira de même pour les systèmes de contrôle de sécurité de sites Web : la vérification Captcha pour distinguer les humains des robots sera remplacée par des modes de web-mining, et il ne sera plus question de savoir si un visiteur est un robot ou un humain puisqu'il « paiera » avec le minage.

La chute des ICO (« Initial Coin Offering »)

Les ICO correspondent au crowdfunding en cryptomonnaies. En 2017, cette approche s'est énormément développée avec plus de 3 milliards de dollars recueillis par divers projets, la plupart liés d'une façon ou d'une autre aux blockchains. L'année prochaine, nous nous attendons à ce que l'hystérie autour des ICO décline, avec une série d'échecs (incapacité à créer les produits financés par les ICO) et une sélection plus rigoureuse des projets d'investissement. Un certain nombre d'échecs de projets ICO peuvent affecter négativement le taux de change des cryptomonnaies (Ethereum, Bitcoin, etc.), qui, en 2017, avaient connu une croissance sans précédent. Nous pourrons ainsi voir une diminution du nombre absolu d'attaques de phishing et de piratage ciblant les ICO, les contrats intelligents et les porte-monnaie.

CONCLUSION

Les technologies connectées ont le pouvoir de rendre la vie plus agréable et plus sûre, mais elles apportent avec elles de nouvelles vulnérabilités que les cyberattaquants seront prompts à exploiter. Comme indiqué au début de ce rapport, ces prévisions sont fondées sur l'expérience et les connaissances acquises au cours de la dernière année par nos chercheurs experts. Il s'agit d'opinions, et toutes ces prévisions ne vont pas forcément se confirmer. Mais il vaut mieux être bien préparé pour la bataille, et le secteur de la sécurité, dont nous sommes une part active, continuera à répondre aux derniers outils et dernières techniques des cybercriminels avec des solutions de sécurité et une threat intelligence toujours meilleures, afin de faire du monde un lieu plus sûr pour tous, sauf pour les criminels.

Securelist, la ressource destinée à la recherche technique, l'analyse et la réflexion des experts de Kaspersky Lab

Blog Kaspersky Lab

Threatpost, l'actualité des menaces

Blog d'Eugene Kaspersky

KASPERSKY lab